

1      **CARLSON LYNCH, LLP**  
2      TODD D. CARPENTER (234464)  
3      1350 Columbia Street, Suite 603  
4      San Diego, CA 92101  
5      Tel: 619-762-1910  
6      Fax: 619-756-6991  
7      tcarpenter@carlsonlynch.com

8      *Attorneys for Plaintiffs and the Proposed Class*

9      [Additional counsel listed on signature page.]

10     **UNITED STATES DISTRICT COURT**  
11     **NORTHERN DISTRICT OF CALIFORNIA**  
12     **OAKLAND DIVISION**

13     KELLY WHALEN, Individually and on Behalf of  
14     All Others Similarly Situated, and S.M., a Minor,  
15     By and Through Her Guardian, Tachah Wade,  
16     Individually and on Behalf of All Others Similarly  
17     Situated,

18     Plaintiffs,

19     v.

20     FACEBOOK, INC.,

21     Defendant.

22     Case No. 4:20-cv-06361-JST

23     **FIRST AMENDED CLASS ACTION**  
24     **COMPLAINT**

25     **DEMAND FOR JURY TRIAL**

26     Plaintiffs Kelly Whalen and S.M., a minor, by and through her guardian Tachah Wade,  
27     individually and on behalf of all others similarly situated, through undersigned counsel, bring this  
28     Class Action Complaint for Violations of the Illinois Biometric Information Privacy Act (“BIPA”),  
29     740 ILCS 14/1, *et seq.*, against Defendant Facebook, Inc. (“Facebook” or “Defendant”), and allege  
30     the following upon information and belief, except as to the allegations within Plaintiffs’ personal  
31     knowledge. Plaintiffs believe that substantial additional evidentiary support will exist for the  
32     allegations set forth herein after a reasonable opportunity for discovery.

33     **I. SUMMARY OF THE ACTION**

34     1. Facebook, Inc. is a social media conglomerate founded in 2004. It owns its eponymous  
35     social networking platform in addition to a host of subsidiaries.

1       2.     Instagram is a photo and video-sharing social networking service that is owned by  
 2 Facebook, Inc. It was initially released as an application for the iOS mobile operating system in 2010  
 3 before being acquired by Facebook in 2012. Since its acquisition by Facebook, Instagram has steadily  
 4 amassed new users worldwide. In 2019, there were more than approximately 118 million users in the  
 5 United States alone.

6       3.     Facebook's social media platform offers a multi-faceted approach for users to connect  
 7 with one another. In addition to sharing photos and videos, Facebook is a social networking service,  
 8 which allows users to share news articles, create special interest groups, shop, and more. Instagram,  
 9 on the other hand, is more limited in its scope of use. Its primary features are photo and video sharing,  
 10 direct messaging, and "stories," which are photos and/or videos that disappear from a user's profile  
 11 after 24 hours.

12      4.     Facebook holds the largest facial dataset to date, powered by DeepFace, Facebook's  
 13 deep-learning facial recognition system, which collects information about face geometry.<sup>1</sup> Based on  
 14 testing, the DeepFace facial recognition system closely approaches human-level accuracy in  
 15 identifying faces. Unless a user opts out, Facebook scans photos uploaded to the social network in  
 16 search of faces it recognizes using its DeepFace technology.<sup>2</sup>

17      5.     Earlier this year, Facebook agreed to pay \$650 million to settle a class action that  
 18 accuses the company of illegally harvesting the protected biometrics of users of its Facebook platform.  
 19 As part of the settlement, Facebook agreed to delete face templates of users that it had created and  
 20 stored.

21      6.     As set forth below, Facebook also illegally harvests the protected biometrics of users  
 22 of its Instagram application. In direct violation of Sections 15(b)-(e) of the BIPA, Facebook is actively  
 23 collecting, storing, disclosing, profiting from, and otherwise using the biometric data of its reportedly  
 24 more than 100 million Instagram users, which includes millions of Illinois residents, without any  
 25 written notice or informed written consent.

26  
 27      

---

<sup>1</sup> <https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/>

28      <sup>2</sup> <https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html>

1       7.     Facebook has readily admitted to its collection of biometrics from users. As explained  
 2 by Facebook, its use of face recognition technology includes analyzing uploaded photos and videos it  
 3 thinks a user may appear in on Facebook, such as a user's profile picture, as well as photos and videos  
 4 that he/she has been tagged in, and then creates a unique number for that user, called a template.<sup>3</sup>

5       8.     Its facial recognition software works by scanning faces of unnamed people in photos  
 6 and videos to analyze details of individuals' faces, checking whether they match with those for whom  
 7 Facebook has already created templates. While Facebook claims that users are in charge of that  
 8 process, in reality, people cannot actually control the technology because Facebook scans their faces  
 9 in photos and videos uploaded by *other* users even if their individual facial recognition setting is  
 10 turned off.<sup>4</sup>

11      9.     Facebook claims it uses an individual's template to find photos and videos a user  
 12 appears in, to suggest tags, and to provide more relevant content and feature recommendations.<sup>5</sup>  
 13 Facebook also surreptitiously captures its Instagram users' protected biometrics without their  
 14 informed consent and, worse yet, without actually informing users of its practice. Upon information  
 15 and belief, once Facebook captures its Instagram users' protected biometrics, it associates this data  
 16 with an existing Facebook template and/or includes this data in its dataset of biometrics that it uses to  
 17 power, train, and develop its facial recognition software. Moreover, it then uses this biometric data  
 18 for its own business and financial gain, including, but not limited to, bolstering its facial recognition  
 19 abilities across all of its products, including the Facebook application and sharing this information  
 20 among various entities. Facebook does all of this without providing any of the required notices or  
 21 disclosures required by Illinois' BIPA.

22      10.    Plaintiffs bring this action individually and on behalf of a proposed class in order to  
 23 stop Facebook's violations of the BIPA and to recover statuary damages for Facebook's unauthorized  
 24 collection, storage, disclosure, profiting from, and use of their biometric data in violation of the BIPA.

25  
 26  
 27     <sup>3</sup> <https://www.facebook.com/help/122175507864081>

28     <sup>4</sup> <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html>

29     <sup>5</sup> <https://www.facebook.com/help/122175507864081>

1       **II. PARTIES**

2       11. Plaintiff Kelly Whalen is, and has been at all relevant times, a resident and citizen of  
 3 the state of Illinois and a resident of Cook County, Illinois. Plaintiff Whalen first created an Instagram  
 4 account on November 17, 2011 and has used Instagram regularly since that time.

5       12. During the relevant time period, Ms. Whalen accessed Instagram on both her computer  
 6 and phone to post photographs, view content posted by other users, and react to that content via  
 7 comments and “likes.” Ms. Whalen frequently tagged herself and others in photographs posted on  
 8 Instagram, and appeared in photographs uploaded by others to Instagram. Ms. Whalen was not aware  
 9 that any facial recognition data or other biometric data was being collected by Facebook through her  
 10 Instagram use.

11       13. S.M., by and through her guardian, Tachah Wade (her mother), is a minor child and a  
 12 resident and citizen of the state of Illinois and a resident of Kendall County, Illinois. S.M. is the owner  
 13 of an Instagram account which includes content she has posted.

14       14. During the relevant time period, S.M. accessed Instagram on her phone to post  
 15 photographs, view content posted by other users, and react to that content via comments and “likes.”  
 16 In addition to photographs of herself that she uploaded to her account, S.M. was frequently tagged in  
 17 photographs uploaded by others to Instagram.

18       15. Defendant Facebook is a Delaware corporation with its headquarters and principal  
 19 executive offices at 1601 Willow Road, Menlo Park, California 94025. Facebook is a citizen of the  
 20 states of Delaware and California. Facebook is also registered to conduct business in the State of  
 21 Illinois (file number 66267067) and maintains an office in Cook County, Illinois.

22       **III. JURISDICTION AND VENUE**

23       16. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the “Class Action  
 24 Fairness Act”) because sufficient diversity of citizenship exists between the parties in this action, the  
 25 aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and there are  
 26 well in excess of 100 class members. Because it is estimated that the Class will have thousands of  
 27 members and Defendant’s intentional and reckless violations of BIPA are punishable by statutory  
 28

1 damages of \$5,000 per violation, the amount in controversy is well in excess of \$5,000,000. This  
 2 Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1337.

3       17. The Court has personal jurisdiction over Defendant because it has affirmatively  
 4 established and maintained sufficient contacts with California in that Defendant is registered to do  
 5 business in this State, is headquartered in this State, and conducts significant business in this State.

6       18. Venue is proper under 28 U.S.C. § 1331(b)(1) because Defendant's principal place of  
 7 business is in this judicial district.

8 **IV. SUBSTANTIVE ALLEGATIONS**

9       **I. Biometric Information and the Illinois BIPA**

10      19. A "biometric identifier" (together with "biometric information,"<sup>6</sup> "biometrics" or  
 11 "biometric data") is any personal feature that is unique to an individual including fingerprints, iris  
 12 scans, DNA, facial features and voice, among others.

13      20. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers  
 14 that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example,  
 15 social security numbers, when compromised, can be changed. Biometrics, however, are biologically  
 16 unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened  
 17 risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

18      21. In recognition of this legitimate concern over the security of biometric data, the Illinois  
 19 Legislature enacted the BIPA, which provides, *inter alia*, that:

20      No private entity may collect, capture, purchase, receive through trade, or otherwise  
 21 obtain a person's or a customer's biometric identifier or biometric information, **unless it first**:

22       **(1) informs** the subject or the subject's legally authorized representative in  
 23 writing that a biometric identifier or biometric information is being collected or  
 24 stored;

25       **(2) informs** the subject or the subject's legally authorized representative in  
 26 writing of the **specific purpose and length of term** for which a biometric identifier or  
 27 biometric information is being collected, stored, and used; **and**

28      

---

 29      <sup>6</sup> The BIPA defines "biometric information" as "any information, regardless of how it is captured,  
 30 converted, stored, or shared, based on an individual's biometric identifier used to identify an  
 31 individual." 740 ILCS 14/10. Plaintiffs herein use the terms "biometric information" and "biometric  
 32 identifier" interchangeably.

(3) receives a **written release** executed by the subject of the biometric identifier or biometric information or the subject's legally authorized **representative**.

740 ILCS 14/15(b).

22. As alleged herein, Facebook's practices of collecting, storing, and using Instagram users' biometric information without informed written consent violates all three prongs of §15(b) of the BIPA.

23. Facebook has also violated Section 15(c) of the BIPA by selling, leasing, trading, or otherwise profiting from a person's biometrics, as set forth more fully below.

24. Facebook has likewise violated Sections 15(d)-(e) of the BIPA by disclosing, rediscovering, or otherwise disseminating the biometrics captured from media uploaded to Instagram, as set forth more fully below.

## II. Facebook Collects, Stores, Discloses, Profits from, and Otherwise Uses Plaintiffs' and Class Members' Biometric Data in Violation of the BIPA

25. Instagram has over one billion users worldwide and millions of users in Illinois alone.

26. Instagram allows its users to create a personal page where users can upload photographs and videos, participate in live video broadcasts, and communicate and interact with other Instagram users. Approximately 95 million photos are shared on Instagram each day, with over 40 billion photos and videos shared on the platform since its inception.

27. Facebook has employed its facial recognition technology continuously from the time it was first introduced in 2010, including the time period after its acquisition of Instagram in 2012, and continuing to the date of the filing of this Complaint.

28. Facebook's sophisticated facial recognition technology works by collecting and analyzing the facial features of individuals appearing in photographs and videos uploaded to its Facebook and generating a "biometric signature" or "face template" of each individual's face that appears therein. This facial template is based on each person's facial geometry and is specific to that person. Facebook, upon information and belief, also collects biometric data from Instagram users. It scans photos, videos, or other content uploaded to Instagram for biometric data. As Facebook's Instagram and Facebook users continue to manually tag friends, family, and other people they

1 recognize in a photograph, Facebook's software automatically compares those images to the face  
 2 templates and other biometrics in its database. If there is a match, Facebook may identify the user.

3       29. Facebook is then able to identify the individuals whose biometrics it has captured by  
 4 cross referencing the biometric data of individuals appearing in Instagram photographs with face  
 5 templates that it has already linked with an identified individual (for instance, the face template  
 6 created for the individual by Facebook or companies with whom Facebook shares captured  
 7 biometrics), and identify the individual when there is a match.

8       30. Prior to January 1, 2020, Facebook has never informed Instagram users that it collects  
 9 their biometric data. Rather, the Instagram Data Policy merely states that Facebook collects  
 10 information "you and others provide" to the app, in the form of both posted content and anything users  
 11 might see through the camera, and that its systems *automatically process* the content and  
 12 communications provided by users *to analyze context and what's in them* (emphasis added).<sup>7</sup>

13       31. In fact, Facebook actively mislead Instagram users about whether it was collecting  
 14 facial recognition data. Instagram's Data Policy states, "**If you have it turned on, we use face**  
 15 **recognition technology to recognize you in photos, videos and camera experiences.**"<sup>8</sup> However,  
 16 Instagram users have no ability to turn off any facial recognition software within the app. Furthermore,  
 17 the Instagram Data Policy states, "If we introduce face-recognition technology to your Instagram  
 18 experience, we will let you know first, and you will have control over whether we use this technology  
 19 for you."<sup>9</sup> As set forth below, these statements are untrue.

20       32. On January 1, 2020, Facebook published, for the first time, its California Privacy  
 21 Notice for its California users as a supplement to its current Data Policy in compliance with  
 22 California's Consumer Privacy Act (CCPA).<sup>10</sup> Instagram admits in this notice that any of the  
 23 information disclosed within the California Privacy Notice may have been collected from users over  
 24 the past 12 months. While California is currently the only state requiring these types of disclosures to

25  
 26 <sup>7</sup> See <https://help.instagram.com/155833707900388> Section I: What Kinds of Information Do We  
 27 Collect?

<sup>8</sup> See <https://help.instagram.com/519522125107875> Section II: How Do We Use This Information?

<sup>9</sup> *Id.*

<sup>10</sup> See <https://help.instagram.com/2482657248648591> "California Privacy Notice"

1 consumers, the content of the notice demonstrates that Facebook has been collecting biometric data  
 2 from its Instagram users for, at minimum, the 2019 calendar year. The California Privacy Notice is  
 3 reproduced in part below (emphasis added):

4 5 Categories of Personal Information we collect may include:	6 7 8 9 Examples of how Personal Information is used include:	10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 Parties with whom your information may be shared include:
<ul style="list-style-type: none"> <li>• <b><i>Identifiers</i></b>;</li> <li>• Data with special protections, if you choose to provide it;</li> <li>• Commercial information, if you choose to provide it;</li> <li>• <b><i>Photos and face imagery that can be used to create face-recognition templates if you or others choose to provide it and you have the setting turned on</i></b>.</li> <li>• Internet or other electronic network activity information, including content you view or engage with;</li> <li>• Location-related information, including precise device location if you choose to allow us to collect it;</li> <li>• <b><i>Audio or visual Information, including photos and videos, if you or others choose to provide it</i></b>;</li> <li>• Professional or employment information, if you choose to provide it;</li> <li>• Education information, if you choose to provide it;</li> <li>• Financial information, if you choose to provide it; and</li> <li>• Information derived from other Personal Information about you, which could include your preferences, interests, and other information used to personalize your experience.</li> </ul>	<ul style="list-style-type: none"> <li>• Providing, personalizing, and improving our Products;</li> <li>• Facilitating transactions, providing measurement, analytics, advertising, and other business services;</li> <li>• Promoting safety, integrity, and security;</li> <li>• Communicating with you;</li> <li>• Researching and innovating for social good; and</li> <li>• To perform other business purposes.</li> </ul>	<ul style="list-style-type: none"> <li>• People and accounts you share and communicate with;</li> <li>• People and accounts with which others share or reshare content about you;</li> <li>• Apps, websites, and third-party integrations on or using our Products;</li> <li>• New owners in the event of a change of ownership or control of all or part of our Products or their assets changes;</li> <li>• Partners, including partners who use our analytics services, advertisers, measurement partners, partners offering goods and services in our Products, vendors and service providers, and researchers and academics;</li> <li>• Law enforcement or other third parties in connection with legal requests; and</li> <li>• Facebook Companies.</li> </ul>

1       33. Although Facebook's California Privacy Notice indicates that it collects Instagram  
 2 users' protected biometrics "if you or others choose to provide it and you have the setting turned on,"  
 3 Facebook's belated, after-the-fact notice to Instagram users cannot constitute compliance with the  
 4 BIPA for a variety of reasons, including that Facebook only allowed Class Members to opt out *after*  
 5 it collected their protected biometrics, and even then, only if Class Members knew to look for the opt-  
 6 out option, which, upon information and belief, is not even possible through a user's *Instagram*  
 7 account.<sup>11</sup>

8       34. In any event, Instagram users *cannot* opt out. Indeed, Instagram users are not even  
 9 given an opportunity to provide a written release because Facebook automatically processes content  
 10 and shares it across its platforms. Rochelle Nadhiri, a Facebook spokeswoman, said its system  
 11 analyzes faces in users' photos to check whether they match with those who have their facial  
 12 recognition setting turned on. This means that users can never really "opt out" of Facebook's use of  
 13 facial recognition. So even if a user does not have facial recognition activated within their personal  
 14 account, their photo may still be scanned, collected, and entered into Facebook's database if it matches  
 15 with a user's data who does have the facial recognition setting activated.<sup>12</sup> This also means that one  
 16 can never truly "opt out" because Facebook must capture and compare the biometrics of a face before  
 17 learning if that face, in fact, matches with faces of users who have their facial recognition setting  
 18 turned on or off.

19       35. Further, Facebook concedes that it collects information such as the location of a photo,  
 20 Instagram users' current location, where they live, the places they go, and the businesses and people  
 21 they are near to "provide, personalize and improve our Products." As such, Facebook knows, or  
 22 should know, that Plaintiffs and Class Members are Illinois users.<sup>13</sup>

23       36. Moreover, upon information and belief, Facebook disclosed Instagram users'  
 24 biometric data not only across teams operating across its own various platforms, but also with third  
 25 parties. Facebook concedes that biometrics harvested from Instagram's photographs and videos may  
 26

---

27       <sup>11</sup> See <https://help.instagram.com/519522125107875>, directing Instagram users to "opt out" via settings  
 on their *Facebook* profile.

28       <sup>12</sup> See <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html>

13 See <https://help.instagram.com/155833707900388>

1 be shared with other apps, websites, and third-party integrations, Facebook's partners, including  
 2 partners who use Facebook's analytics services, advertisers, measurement partners, partners offering  
 3 goods and services within Facebook's products, vendors and service providers, researchers and  
 4 academics, law enforcement, and Facebook Companies, including Facebook Payments Inc., Onavo,  
 5 Facebook Technologies, LLC and Facebook Technologies Ireland Limited, WhatsApp Inc.,  
 6 WhatsApp Ireland Limited, and CrowdTangle.<sup>14</sup>

7 37. Facebook and Instagram share infrastructure, systems, and technology with other  
 8 Facebook Companies and process information about the user across the Facebook Companies.<sup>15</sup> This  
 9 includes, upon information and belief, using Facebook's facial recognition technology to process  
 10 biometrics collected from Instagram users, which are then used to enhance already-existing facial  
 11 templates of those users.

12 38. For example, Facebook is currently the subject of antitrust litigation in Germany,  
 13 where they are alleged to have broken competition laws by combining personal data collected about  
 14 users across its different platforms, including Instagram, to create "super profiles" for users.<sup>16</sup> A  
 15 ruling from German regulators prohibited Facebook from combining Facebook user account data with  
 16 user data on company services like WhatsApp and Instagram.<sup>17</sup>

17 39. Upon information and belief, Facebook's shared infrastructure, systems, and  
 18 technology and processing of user information across the Facebook Companies includes using the  
 19 biometrics harvested from its Instagram's users' uploaded material to improve the algorithms that  
 20 power its facial recognition abilities across all of its platforms, including, but not limited to, its  
 21 Facebook application where, for example, Facebook uses its facial recognition to suggest tags to  
 22 Facebook users and lets Facebook users know when their photos are uploaded by someone else.<sup>18</sup>

23  
 24  
 25 <sup>14</sup> See <https://help.instagram.com/2482657248648591>

26 <sup>15</sup> See <https://help.instagram.com/155833707900388> Section IV: How Do the Facebook Companies  
 27 Work Together?

28 <sup>16</sup> See <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html>

<sup>17</sup> See <https://www.nytimes.com/2019/02/07/technology/germany-facebook-data.html>

<sup>18</sup> See <https://www.facebook.com/help/122175507864081> What is the face recognition setting on  
 Facebook and how does it work?

1       40. Upon information and belief, Facebook also includes the biometrics captured from  
 2 Instagram users' uploaded material, as well as Instagram users' tagging information, to bolster its  
 3 databases of biometrics, face templates, and tagging information that enables Facebook's facial  
 4 recognition to continue learning and improving, which in turn enhances all of Facebook's facial  
 5 recognition products, including, for example, its predictive tagging feature on the Facebook  
 6 application.<sup>19</sup> Several of Facebook's products, such as Moments, an application Facebook introduced  
 7 in 2015, capitalizes on Facebook's facial recognition technology.<sup>20</sup>

8       41. Several of Facebook's prior patent filings further attest to Facebook's commercial  
 9 purposes in developing its facial recognition technologies. These patents reportedly described one  
 10 system that could detect consumers within stores and match those shoppers' faces with their social  
 11 networking profiles, and another in which cameras near checkout counters could capture shoppers'  
 12 faces and match them with their social networking profiles.<sup>21</sup>

13       42. As such, Facebook profits from its use of its Instagram users' protected biometrics by  
 14 using them to improve the accuracy of its own facial recognition services, to expand the datasets  
 15 which enable its facial recognition software, and to cement its market-leading position in facial  
 16 recognition and social media.

17       43. Accordingly, Facebook and Instagram have collected, captured, or otherwise obtained  
 18 Instagram users' biometric identifiers or biometric information, as those terms are defined in Section  
 19 10 of BIPA, from content that Instagram users uploaded to Instagram.

20       44. Facebook and Instagram are in possession of Instagram users' biometric identifiers or  
 21 biometric information from content that Instagram users uploaded to Instagram.

22       45. Facebook and Instagram scan photographs, videos, or other content uploaded to  
 23 Instagram for biometric identifiers or biometric information.

24

---

25       <sup>19</sup> See <https://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebook-s-facial-recognition-software-is-different-from-the-fbis-heres-why#:~:text=Facebook-,Facebook's%20Moments%20app%20uses%20facial%20recognition%20technology%20to%20group%20photos,friends%20who%20are%20in%20them,&text=When%20someone%20tags%20you%20in,reminder%20of%20a%20shared%20memory.>  
 26 (describing the benefit to facial recognition algorithms of additional photographs and tagging information).

27

28       <sup>20</sup> See <https://techcrunch.com/2015/06/15/facial-recogbook/>

29       <sup>21</sup> See <https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html>

1       46.    In direct contravention of §15(b) of the BIPA, Facebook collected Plaintiffs' and Class  
 2 Members' biometrics without informing them that it would collect, store, and use their biometric  
 3 facial data, without informing Instagram users of the specific purpose and length of term for which  
 4 their biometric data would be collected, stored, and used, and without receiving a written release from  
 5 Instagram users before it began to collect, store, disclose, profit from, and otherwise use their  
 6 biometric data.

7       47.    In direct contravention of §15(c) of the BIPA, Facebook profited from Plaintiffs' and  
 8 Class Members' protected biometrics.

9       48.    In direct contravention of §15(d)-(e) of the BIPA, Facebook voluntarily disclosed and  
 10 otherwise disseminated Plaintiffs' and Class Members' protected biometrics.

11       **III. Plaintiffs' and Class Members' Injuries and Damages**

12       49.    As alleged herein, as a result of Facebook's unlawful conduct, Plaintiffs and Class  
 13 Members have already sustained injuries and face many more imminent and certainly impending  
 14 injuries, which they will continue to suffer.

15       50.    Facebook's unlawful conduct has resulted in, among other injuries: (a) Plaintiffs' and  
 16 Class Members' unique biometric identifiers and information being collected, captured, obtained,  
 17 disclosed, and otherwise disseminated without the requisite notice having been given and without the  
 18 requisite releases having been obtained; and (b) Plaintiffs and Class Members being deprived of the  
 19 very control over their biometric identifiers and information that BIPA was designed to protect.

20       51.    To this day, Plaintiffs and Class Members do not know which, or how many,  
 21 individuals or entities have received, obtained, accessed, stored, disclosed, or otherwise made use of  
 22 Plaintiffs' and Class Members' biometric identifiers and information, exposing them to the imminent  
 23 and certainly impending injuries of identity theft, fraud, stalking, surveillance, social engineering, and  
 24 other invasions of privacy.<sup>22</sup>

25       52.    As a result of Facebook's misconduct, Plaintiffs and Class Members have no recourse  
 26 for the fact that their biologically unique information has been compromised. Moreover, Plaintiffs  
 27

---

28       <sup>22</sup> *Facial Recognition Tech: 10 Views on Risks and Rewards*, <https://www.forbes.com/sites/forbestechcouncil/2018/04/03/facial-recognition-tech-10-views-on-risks-and-rewards/#54d3e1716b3c>

1 and Class Members are likely to withdraw from biometric-facilitated transactions and other facially-  
 2 mediated electronic participation.

3 **IV. Plaintiffs' Personal Experiences**

4 53. Ms. Whalen is a resident of Palos Heights, Illinois. Ms. Whalen signed up for an  
 5 Instagram account in Palos Heights, Illinois in 2011, and has since then uploaded numerous  
 6 photographs.

7 54. Since joining Instagram, Ms. Whalen has uploaded and posted many photographs to  
 8 Facebook's network from Instagram that include images of her face, and Ms. Whalen has tagged  
 9 herself in many of those photographs. Ms. Whalen's face has also appeared in many photographs that  
 10 other Instagram users have uploaded to Instagram, and Ms. Whalen's face has been tagged by other  
 11 Instagram users in many such photographs.

12 55. Many of these photographs were taken in Illinois and were uploaded to Ms. Whalen's  
 13 account from her computer in Illinois.

14 56. S.M. is a resident of Yorkville, Illinois. S.M. signed up for her Instagram account in  
 15 Yorkville, Illinois.

16 57. Since joining Instagram, S.M. has posted photographs and videos to Facebook's  
 17 network from Instagram that include images of her face. She has also been tagged in photographs that  
 18 other Instagram users have uploaded to Instagram.

19 58. As is the case for Class Members, Facebook has, upon information and belief, captured  
 20 biometric identifiers and information from Plaintiffs' photographs by automatically locating and  
 21 scanning Plaintiffs' faces, and by extracting geometric data relating to the contours of their faces and  
 22 the distances between their eyes, nose, and ears -- data which Facebook then collected and stored, as  
 23 set forth more fully below.

24 59. The biometric data collected from Plaintiffs, upon information and belief, was stored  
 25 and used by Facebook for research purposes to develop its own facial recognition technologies across  
 26 the various services and products it offers in connection with its Facebook Companies, including its  
 27 advertising services. Facebook stores, discloses, profits from, and otherwise uses Plaintiffs'  
 28 biometrics without their knowledge or consent.

1       60. Plaintiffs did not receive notice that Facebook would collect, store, profit from,  
 2 disclose, or otherwise use their biometric data when they used the Instagram app.

3       61. Facebook never sought – and Plaintiffs never provided – informed consent, in writing  
 4 or otherwise, to Facebook’s collection, creation, storage, or use of their biometric data.

5       62. Plaintiffs accordingly were never provided an opportunity to prohibit or prevent  
 6 Facebook from collecting, storing, disclosing, profiting from, or otherwise using their protected  
 7 biometrics.

8 **V. CLASS ACTION ALLEGATIONS**

9       63. Plaintiffs bring this lawsuit on behalf of the following proposed class (the “Class”)  
 10 under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the  
 11 following Class, defined as follows:

12       *All Instagram users living in Illinois who had their biometric information or  
 13 identifiers, including scans of their face geometry, collected, captured, received or  
 otherwise obtained by Facebook through materials uploaded to the Instagram  
 14 application.*

15       64. Subject to additional information obtained through further investigation and discovery,  
 16 the foregoing definition of the Class may be expanded or narrowed by amendment or amended  
 17 complaint.

18       65. Specifically excluded from the Class are Defendant, its officers, directors, agents,  
 19 trustees, parents, children, corporations, trusts, representatives, employees, principals, servants,  
 20 partners, joint-venturers, or any entities controlled by Defendant, and its heirs, successors, assigns, or  
 21 other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the  
 22 judge assigned to this action, and any member of the judge’s staff and immediate family.

23       66. **Numerosity.** The members of the Class are so numerous that individual joinder is  
 24 impracticable. Upon information and belief, Plaintiffs allege that the Class contains many thousands  
 25 of members. Although the precise number of Class members is unknown to Plaintiffs, the true number  
 26 of Class members is known by Defendant, and thus, may be notified of the pendency of this action by  
 27 first class mail, electronic mail and/or published notice.

1       67. *Existence and predominance of common questions of law and fact.* Common  
 2 questions of law and fact exist as to all members of the Class and predominate over any questions  
 3 affecting only individual Class members. These common legal and factual questions include, but are  
 4 not limited to, the following:

- 5               (a) whether Defendant collected, captured, received, or otherwise obtained  
 6 biometric identifiers or biometric information from Plaintiffs and the Class;
- 7               (b) whether Defendant informed Plaintiffs and the Class before collecting, using,  
 8 and storing their biometric identifiers or biometric information, as required by §15(b) the  
 9 BIPA;
- 10               (c) whether Defendant informed Plaintiffs and the Class of the specific purpose and  
 11 length of term for which a biometric identifier or biometric information is being collected, stored  
 12 and used, as required by §15(b) the BIPA;
- 13               (d) whether Defendant obtained a written release, as defined by the BIPA, from  
 14 Plaintiffs and the Class to collect, store, and use their biometric identifiers or biometric  
 15 information;
- 16               (e) whether Defendant used biometric data to identify Plaintiffs and the Class;
- 17               (f) whether Defendant sold, leased, traded, or otherwise profited from Plaintiffs'  
 18 or Class Members' biometric identifiers and biometric information in violation of §15(c) of  
 19 the BIPA;
- 20               (g) whether Defendant disclosed, redisclosed, or otherwise disseminated  
 21 Plaintiffs' and Class Members' biometric identifiers or biometric information in violation of  
 22 §15(d) of the BIPA;
- 23               (h) whether Defendant protected Plaintiffs' and Class Members' biometric  
 24 identifiers or biometric information from disclosure pursuant as required by §15(e) of the  
 25 BIPA;
- 26               (i) whether Defendant's violations of the BIPA were committed intentionally,  
 27 recklessly or negligently;

(j) whether Plaintiffs and the Class are entitled to statutory damages under the BIPA and the correct measure of those damages; and

(k) whether Plaintiffs and the Class are entitled to declaratory and injunctive relief.

68. ***Typicality.*** Plaintiffs' claims are typical of the claims of the other members of the Class Defendant collected, stored, and used her biometrics without informed consent in the exact manner as every other Class member.

69. *Adequacy of representation.* Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel highly experienced in complex consumer class action litigation, and Plaintiffs intend to vigorously prosecute this action. Further, Plaintiffs have no interests that are antagonistic to those of the Class.

70. ***Superiority.*** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs committed against them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

71. The Class may also be certified because:

(a) the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication with respect to individual Class members that would establish incompatible standards of conduct for the Defendant;

(b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of

1 the interests of other Class members not parties to the adjudications, or substantially impair or  
2 impede their ability to protect their interests; and/or

3 (c) Defendant has acted or refused to act on grounds generally applicable to the  
4 Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with  
5 respect to the members of the Class as a whole.

6 **COUNT I**

7 **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b)**  
8 **(On Behalf of Plaintiffs and the Class)**

9 72. Plaintiffs reallege and incorporate by reference the allegations contained in the  
10 preceding paragraphs as though fully set forth herein.

11 73. Section 15(b) of the BIPA provides that a private entity may not, among other things,  
12 collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's  
13 biometric identifiers or biometric information, unless it first:

14 (1) informs the subject . . . in writing that a biometric identifier or  
15 biometric information is being collected or stored;

16 (2) informs the subject . . . in writing of the specific purpose and length of  
17 term for which a biometric identifier or biometric information is being collected,  
18 stored, and used; and

19 (3) receives a written release executed by the subject of the biometric  
20 identifier or biometric information . . .

21 740 ILCS 14/15(b).

22 74. Facebook is a private entity under the BIPA. *See* 740 ILCS 14/10.

23 75. Plaintiffs and the Class members are individuals under the BIPA. *See id.*

24 76. Facebook collected Plaintiffs' and the Class members' biometric information and  
25 biometric identifiers as alleged above. *See id.*

26 77. Facebook systematically collected, used, and stored Plaintiffs' and the Class members'  
27 biometric identifiers and biometric information without first obtaining the written release required by  
28 §15(b) of the BIPA.

1       78.     As alleged above, Facebook did not inform Plaintiffs or the Class members in writing  
 2 that their biometric identifiers or biometric information were being collected, stored and used, as  
 3 required by §15(b) of the BIPA.

4       79.     As alleged above, Facebook did not inform Plaintiffs or the Class members in writing  
 5 of the specific purpose and length of term for which their biometric identifiers or biometric  
 6 information was being collected, stored and used, as required by §15(b) of the BIPA.

7       80.     By collecting, storing, and using Plaintiffs' and the Class members' biometric  
 8 identifiers and biometric information as described herein, Facebook violated Plaintiffs' and the Class  
 9 members' rights to privacy in their biometric identifiers or biometric information, as set forth in the  
 10 BIPA, 740 ILCS 14/1, *et seq.*

11       81.     Facebook's violations of §15(b) of the BIPA were intentional or reckless because  
 12 Facebook collected biometric data by default and without written notice as required by the BIPA and,  
 13 therefore, Plaintiffs and the Class members had no opportunity to provide Defendant with a written  
 14 release, as mandated by the BIPA. Alternatively, Facebook's violations of §15(b) of the BIPA were  
 15 negligent because Facebook failed to meet the applicable standard of care in ensuring that its members  
 16 were informed and consented to the collection, storage, and use of their biometric information and  
 17 biometric identifiers.

18       82.     As a result of Defendant's violations of §15(b) of the BIPA, Plaintiffs seek the  
 19 following relief individually and on behalf of the Class: (1) injunctive and equitable relief pursuant to  
 20 740 ILCS 14/20(4) requiring Facebook to comply with the BIPA's requirements for the collection,  
 21 storage, and use of biometric identifiers and biometric information as alleged herein; (2) statutory  
 22 damages of \$5,000 for each intentional or reckless violation of the BIPA pursuant to 740 ILCS  
 23 14/20(2), or alternatively, statutory damages of \$1,000 per negligent violation of the BIPA pursuant  
 24 to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees and costs expenses pursuant to 740 ILCS  
 25 14/20(3).

26       ///

27       ///

## COUNT II

**Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(c)  
(On Behalf of Plaintiffs and the Class)**

83. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

84. Section 15(c) of the BIPA provides “[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.”

85. As alleged above, Facebook violated the BIPA by unlawfully profiting from individuals' biometric identifiers and biometric information, including the biometric identifiers and information of Plaintiffs and Class Members.

86. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

87. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

88. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

89. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Member's biometric identifiers and information.

90. Plaintiffs and Class Members also seek punitive damages, injunctive relief, and the reasonable attorneys' fees, costs, and expenses relating to this action.

111

## COUNT III

## **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d) (On Behalf of Plaintiffs and the Class)**

91. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

92. Section 15(d) of the BIPA provides that “[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person’s or a customer’s biometric identifier or biometric information [...].”

93. As alleged above, Facebook violated BIPA by disclosing and otherwise disseminating, upon information and belief, individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiffs and Class Member, even though: (a) neither the subjects of the biometric identifiers and information nor their authorized representatives consented to the disclosure; (b) the disclosure did not complete a financial transaction requested or authorized by the subjects of the biometric identifiers and information or their authorized representatives; (c) the disclosure was not required by State or federal law or municipal ordinance; and (d) the disclosure and redisclosure was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

94. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

95. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

96. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

97. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Member's biometric identifiers and information.

98. Plaintiffs and Class Members also seek punitive damages, injunctive relief, and the reasonable attorney fees, costs, and expenses relating to this action.

**COUNT IV**

## **Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(e) (On Behalf of Plaintiffs and the Class)**

99. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

100. Section 15(e) of the BIPA provides that “[a] private entity in possession of a biometric identifier or biometric information shall:”

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

101. As alleged above, upon information and belief, Facebook violated the BIPA because, while in possession of Plaintiffs' and Class Members' biometric identifiers and information, it failed to protect from disclosure those biometric identifiers and information: (a) using the reasonable standard of care within Facebook industry; and (b) in a manner that is the same as or more protective than the manner in which Facebook protects and protected other confidential and sensitive information when it voluntarily disclosed the biometrics to third parties.

102. Facebook's violations of the BIPA were intentional and reckless or, pleaded in the alternative, negligent.

103. As a direct and proximate result of Facebook's violations of the BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

104. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

105. Unless and until enjoined and restrained by order of this Court, Facebook's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that

1 their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs  
2 and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary  
3 damages will not end the misuse of Plaintiffs' and Class Member's biometric identifiers and  
4 information.

5 106. Plaintiffs and Class Members also seek punitive damages, injunctive relief, and the  
6 reasonable attorney fees, costs, and expenses relating to this action.

7 **COUNT V**

8 **Unjust Enrichment**  
9 **(On Behalf of Plaintiffs and the Class)**

10 107. Plaintiffs reallege and incorporate by reference the allegations contained in the  
11 preceding paragraphs as though fully set forth herein.

12 108. Facebook obtained a monetary benefit from Plaintiffs and Class Members to their  
13 detriment. Facebook did so by profiting off of the covert and unauthorized collection of the biometric  
14 identifiers and information of Plaintiffs and Class Members, while exposing Plaintiffs and Class  
15 Members to a heightened risk of privacy harms and depriving them of their control over their  
16 biometric data.

17 109. Plaintiffs and Class Members did not authorize Facebook to collect, capture, obtain,  
18 disclose, redisclose, disseminate and otherwise profit off from their biometric identifiers and  
19 information.

20 110. Facebook appreciated, accepted, and retained the benefit bestowed upon it under  
21 inequitable and unjust circumstances arising from Facebook's conduct toward Plaintiffs and Class  
22 Members as described herein.

23 111. Facebook sold, leased, traded, and/or otherwise profited from Plaintiffs' and Class  
24 Members' biometric identifiers and information and did not provide full compensation for the benefit  
25 received from Plaintiffs and Class Members.

26 112. Facebook acquired and caused to be acquired Plaintiffs' and Class Members' biometric  
27 identifiers and information through inequitable means in that it collected, captured and otherwise  
28

1 obtained biometric data from Plaintiffs' and Class Members' online photos without permission and  
2 in violation of Illinois law.

3 113. Plaintiffs and Class Members have no adequate remedy at law.

4 114. Under the circumstances, it would be unjust and unfair for Facebook to be permitted  
5 to retain any of the benefits obtained from Plaintiffs and Class Members and their biometric identifiers  
6 and information.

7 115. Under the principles of equity and good conscience, Facebook should not be permitted  
8 to retain the biometric identifiers and information belonging to Plaintiffs and Class Members because  
9 Facebook unlawfully obtained the biometric identifiers and information.

10 116. Facebook should be compelled to disgorge into a common fund or constructive trust,  
11 for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received as a result of its  
12 collection, capture, obtainment, disclosure, redisclosure, dissemination and profiting off of Plaintiffs'  
13 and Class Members' biometric identifiers and information, including but not limited to the value of  
14 the intellectual property derived therefrom.

15 **VI. PRAYER FOR RELIEF**

16 WHEREFORE, Plaintiffs pray for a judgment against Defendant as follows:

17 A. Certifying the Class as defined above, appointing Plaintiffs as Class Representatives,  
18 and appointing their undersigned counsel as Class counsel;

19 B. Declaring that Defendant's actions, as alleged above, violate Sections 15(b),(c),(d),  
20 and (e) of the BIPA, 740 ILCS 14/1, *et seq.*;

21 C. Awarding statutory damages of \$5,000 for each intentional or reckless violation of the  
22 BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000 per negligent  
23 violation of the BIPA pursuant to 740 ILCS 14/20(1);

24 D. Awarding injunctive and equitable relief pursuant to 740 ILCS 14/20(4) requiring  
25 Facebook to comply with the BIPA by providing a publicly available retention schedule or guidelines  
26 for permanently destroying its users' biometric identifiers and biometric information and forcing  
27 Defendant to stop collecting, storing, and using Plaintiffs' and the Class members' biometric identifiers  
28 and biometric information without first obtaining their informed written consent;

1       E.     An order requiring Facebook to disgorge into a common fund or constructive fund, for  
2 the benefit of Plaintiffs and members of the proposed Class, proceeds that it unjustly received as a  
3 result of its collection, capture, obtainment, disclosure, dissemination, and profiting off of Plaintiffs'  
4 and Class Members' biometric identifiers and information;

5       F.     An award of pre-judgment and post-judgment interest for Plaintiffs and members of  
6 the proposed Class, as permitted by law;

7       G.     Awarding Plaintiffs attorneys' fees and costs pursuant to 740 ILCS 14/20(3); and

8       H.     Awarding any further relief as the Court may deem just and proper.

9 **VII. JURY DEMAND**

10      Plaintiffs hereby demand a jury trial on all issues so triable.

11      Dated: November 18, 2020

**CARLSON LYNCH LLP**

12      By: /s/Todd D. Carpenter

13           Todd D. Carpenter (234464)  
14           1350 Columbia St., Ste. 603  
15           San Diego, CA 92101  
16           Tel.: 619-762-1900  
17           Fax: 619-756-6991  
18           tcarpenter@carlsonlynch.com

19      Kyle A. Shambberg\*  
20      Nicholas R. Lange\*  
21      **CARLSON LYNCH LLP**  
22      111 West Washington Street, Suite 1240  
23      Chicago, IL 60602  
24      Tel.: 312-750-1265  
25      kshambberg@carlsonlynch.com  
26      nlange@carlsonlynch.com

27      Matthew E. Lee\*  
28      Erin J. Ruben\*  
29      **WHITFIELD BRYSON LLP**  
30      900 W. Morgan Street  
31      Raleigh, North Carolina 27603  
32      Telephone: (919) 600-5000  
33      Facsimile: (919) 600-5035  
34      dan@whitfieldbryson.com  
35      matt@whitfieldbryson.com  
36      erin@whitfieldbryson.com

37      \*Pro Hac Vice applications pending

38      *Counsel for Plaintiffs and the Proposed Class*